1964

A development of Sylow's theorem

Jack O. Beamer
Lehigh University

AN ABSTRACT OF

"A DEVELOPMENT OF SYLOW'S THEOREM"

by Jack O. Beamer

Of fundamental importance in the theory and study of finite groups are the theorems of Lagrange and Sylow, two theorems very closely related. In general, the converse of Lagrange's Theorem is not true, that is, given a finite group G of order g and any divisor of g, say h, it does not necessarily follow that there is a subgroup H of G of order h.

After a brief discussion of Lagrange's Theorem, a counter-example (in fact, a system of counter-examples) to the converse of Lagrange's Theorem will be demonstrated. It is here that some elementary theory of permutations is used, along with a few basic results about normal subgroups.

If the finite group G is cyclic or Abelian then the converse of Lagrange's Theorem is true. The subject of Sylow's Theorem is the existence in general of subgroups of order h, where h is any divisor of g, the order of G.

Finally, a short survey of p-groups and some related examples will be made since this is a natural outcome of the discussion of Sylow's Theorem.

A DEVELOPMENT OF SYLOW'S THEOREM

by
Jack O. Beamer

A Thesis
Presented to the Graduate Faculty
of Lehigh University
in Candidacy for the Degree of
Master of Science

Lehigh University
June 1964

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

May 13, 1964
(date)

Gerhard Rayna
Professor in Charge

Everett Pitcher
Head of the Department

Acknowledgements

The author wishes to express his sincere appreciation to Mr. Gerhard Rayna for his advice and assistance in the preparation of this thesis.

Table of Contents

AN ABSTRACT OF

"A DEVELOPMENT OF SYLOW'S THEOREM "

by Jack O. Beamer

Of fundamental importance in the theory and study of finite groups are the theorems of Lagrange and Sylow, two theorems very closely related. In general, the converse of Lagrange's Theorem is not true, that is, given a finite group G of order g and any divisor of g, say h, it does not necessarily follow that there is a subgroup H of G of order h.

After a brief discussion of Lagrange's Theorem, a counter-example (in fact, a system of counter-examples) to the converse of Lagrange's Theorem will be demonstrated. It is here that some elementary theory of permutations is used, along with a few basic results about normal subgroups.

If the finite group G is cyclic or Abelian then the converse of Lagrange's Theorem is true. The subject of Sylow's Theorem is the existence in general of subgroups of order h, where h is any divisor of g, the order of G.

Finally, a short survey of p-groups and some related examples will be made since this is a natural outcome of the discussion of Sylow's Theorem.

CHAPTER 1

LAGRANGE'S THEOREM

To prove Lagrange's Theorem, it is necessary to define the concept of cosets and to establish some of the very basic related results.

DEFINITION 1. Let G be a group and H a subgroup of G. Then a left coset of H, denoted Hx, is the set of all elements hx, where h ranges over all the elements of H and x is some fixed element in G. A right coset xH of H is defined similarly.

This immediately yields the following:

LEMMA 1. Let G be a group and H a subgroup of G. Two left cosets of H in G are either disjoint or identical sets of elements. Also, any left coset of H in G contains the same number of elements as H, if H is finite.

PROOF : Let x and y be any two elements of G, and consider the cosets Hx and Hy. If the cosets have no element in common then there is nothing to prove. Otherwise, suppose z is an element of both Hx and Hy. Then there are elements h_1 and h_2 in H such that $z = h_1x = h_2y$. Hence $x = h_1^{-1}h_2y$ and for all h in H, $hx = (hh_1^{-1}h_2)y$ which implies Hx is contained in Hy. Similarly, Hy is contained in Hx, and thus Hx = Hy.

The second part of the lemma is proved by observing that there is a one-to-one correspondence between H and Hx, defined by associating an element h of H with the element hx of Hx. This establishes that H and Hx have the same number of elements.[3]

The above result is also true for right cosets and is proved in a similar manner. By forming all possible left cosets of a subgroup H of a group G, a partition of G into disjoint cosets is obtained; in

fact, the cosets completely exhaust G. Such a partition is commonly called the left decomposition of G with respect to H, and, if G is finite, it may be expressed in the following form: $G = Hx_1 + Hx_2 + \cdots + Hx_r$. The subgroup H is itself always one of the cosets in such a decomposition since $He = H$, e being the identity of G. A right decomposition of G can be constructed similarly, although in the non-commutative case the right and left decompositions may actually differ. However, the number of distinct cosets in both the right and left decompositions is identical. This is easily verified by noting that the one-to-one mapping of x to x^{-1} carries the left coset Hx into the right coset $x^{-1}H$.

DEFINITION 2. The order of a finite group G is the number of distinct elements in G. The order of any element x of G is the smallest positive integer n such that $x^n = e$, where e is the identity of G.

DEFINITION 3. Let H be a subgroup of group G. The index of H in G is the number of distinct cosets in the right or left decomposition of G with respect to H.

It is now possible to state and prove the following theorem due to Lagrange.

THEOREM 1. The order and the index of every subgroup H of a finite group G are divisors of the order of the group.

PROOF: Let the order of the group G be g and the order of H be h. Form the left decomposition of G with respect to H. Then $G = H + Hx_2 + \cdots + Hx_r$ where $r \leq g$. By Lemma 1 and preceding remarks, $g = hr$, where r is the index of H in G.

CHAPTER 2

COUNTER-EXAMPLE TO THE CONVERSE OF LAGRANGE'S THEOREM

The aim now is to develop a counter-example to the converse of Lagrange's Theorem in general, and then proceed to establish the validity of the converse under certain restrictions.

DEFINITION 4. Let G be a finite group and let H be a subgroup of G. Then H is said to be a normal subgroup of G if the left and right decompositions of H with respect to G coincide.

It is interesting to note that this definition is equivalent to saying that $xH = Hx$ for all x in G. A proof of this equivalence is as follows:

Clearly, $xH = Hx$ for all x in G implies that the right and left decompositions of H with respect to G coincide. On the other hand, suppose $G = Hx_1 + Hx_2 + \dots + Hx_r$ and $G = y_1H + y_2H + \dots + y_rH$. Then for each i, $1 \leq i \leq r$, there is a j, $1 \leq j \leq r$, such that $Hx_i = y_jH$ and x_i does not necessarily equal y_j. Let x be any element of G. Then x belongs to some $Hx_i = y_jH$. Hence there exist elements h_1 and h_2 in H such that $x = h_1x_i = y_jh_2$. Let h' be any element of H. Then $xh' = y_jh_2h'$. But h_2h' is an element of H and hence $y_j(h_2h') \in y_jH = Hx_i$. Thus there is an element h'' in H such that $xh' = h''x_i$. But $x_i = h_1^{-1}x$ and hence $xh' = h''x_i = h''h_1^{-1}x$ implying that $xH = Hx$ for all x in G.

This result is now used to prove the following theorem.

THEOREM 2. Let G be a finite group and H a subgroup of G of index two. Then H is a normal subgroup of G.

PROOF: Since H has index two, both the right and left decompositions of

G with respect to H consist of exactly two distinct cosets. One of these cosets is always H itself, and the remaining coset is necessarily G/H (the complement of H in G) since distinct cosets in a decomposition are disjoint and they completely exhaust G. Thus H and G/H are the disjoint cosets in both the right and left decompositions. This proves that H is a normal subgroup of G.

It is now necessary to digress for several remarks on permutations and some direct consequences.

DEFINITIONS 5. A permutation is a one-to-one mapping of a set onto itself.

Suppose S is any set with n elements, say a, b, ..., n. Then one possible permutation on S may be written $\begin{pmatrix} a & b & \cdots & m & n \\ b & c & \cdots & n & a \end{pmatrix}$, meaning that the mapping transforms a into b, b into c, ..., and n into a. Such a permutation is called a cycle, due to the cyclical displacement of elements, and has an alternative representation in the form (a b ... m n). In this connection, it is an important fact that any permutation that is not itself a cycle is expressible as a product of disjoint cycles. The product of permutations is not in general commutative, that is, multiplication of cycles from left to right results in a different image than that obtained by multiplying the cycles from right to left. Henceforth then it will be assumed, unless otherwise stated, that multiplication is from left to right; that is, that the product of two permutations is the result of first applying the left-hand permutation to the given set of elements, and then applying the right-hand permutation to the image.

It can also be shown that any cycle (abc...mn) can be factored and

written as (ab)(ac)...(am)(an). The number of elements of S in any cycle is said to be the length of that cycle, and cycles of length two are called transpositions. From the preceding remarks then, any permutation can be written as the product of transpositions. A permutation which can be written as the product of an even number of transpositions is said to be an even permutation and a permutation expressible as the product of an odd number of transpositions is defined to be an odd permutation. For example, consider the set consisting of the integers one through five. The permutation $\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$ = (1 2 3 4 5) = (12)(13)(14)(15) is an even permutation, while the permutation $\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}$ = (12)(345) = (12)(34)(35) is odd.

A natural question now arises. Can a permutation, by being capable of being written two ways, be both odd and even? The negative reply will now be established.

DEFINITION 6. Let s be a permutation on the first n positive integers, 1,2,...,n. Let i and j assume values from 1 to n, where $i < j$. Then define P to be the number $\prod_{i<j}(i - j)$ and define P(s) to be the number $\prod_{i<j}(is - js)$, that is the number obtained by performing the permutation s on the elements 1,2,...,n.

Note that if s is an arbitrary permutation, then either P(s) = P or P(s) = -P. In particular, if s is a transposition, then P(s) = -P. The desired result now follows.

THEOREM 3. No permutation is both odd and even.

PROOF: Let s be any permutation. Suppose s is both even and odd. Then $s = a_1a_2\cdots a_k$ and $s = b_1b_2\cdots b_\ell$, where for $1 \leq i \leq k$ and $1 \leq j \leq \ell$, a_i and b_j are transpositions. Without loss of generality, assume k

is an even integer and ℓ is an odd integer. Then from the preceding remarks $P(s) = (-1)^k P = P$, since k is even, and $P(s) = (-1)^\ell P = -P$, since ℓ is odd. But this implies that $P = -P$ since $P(s) = P(s)$. This can only occur for $P = 0$, which is a contradiction since P is, by definition, the product of non-zero factors.

It is not difficult to show that if S is a set with n elements then the set of all permutations on S forms a group, called the symmetric group of degree n and designated by S_n. This group has order $n!$. If n is greater than one, then the alternating group A_n of degree n consists of all the even permutations on S and has order $\frac{n!}{2}$.

One additional definition is needed.

DEFINITION 7. A group G is said to be a simple group if it contains no proper normal subgroups.

THEOREM 4. The alternating group A_n of any degree $n \geq 5$ is simple.

As the proof of this theorem is rather long and tedious, only a general outline of it will be given. The proof consists of three main parts. They are as follows:

(a) Prove that A_n is generated by cycles of length three.

(b) Show that if a normal subgroup of A_n contains one cycle (ijk) of length three, then it contains all cycles of length three.

(c) Show that every normal subgroup of A_n contains at least one cycle of length three. [4]

Many counter-examples to the converse of Lagrange's Theorem are now evident. For example, consider the alternating group A_5 of degree five. The order of A_5 is $\frac{5!}{2} = 60$. One divisor of 60 is 30. But A_5 has no subgroup H of order 30, for if so, H would have index two by Lagrange's

Theorem, implying H is a normal subgroup of A_5 by Lemma 2. But this is in contradiction to the fact that A_5 is simple. In general, no alternating group of degree $n \geq 5$ has any subgroup of order $\frac{n!}{4}$.

CHAPTER 3

THE CYCLIC CASE

There are two different cases to be considered in connection with cyclic groups: one is the case when the order of the group is a prime (p is a prime number if and only if it is divisible only by $\pm$ p and $\pm$ 1), and the other case being a cyclic group of composite order.

DEFINITION 8. A group G is said to be cyclic if every element of G is expressible as a power of some fixed element of G, say a. Such an element a is called a generator or generating element of G and G may then be denoted by $\{a\}$.

It is evident from Lagrange's Theorem that a cyclic group of prime order p has no proper subgroups, since p has no proper divisors. The second case may be disposed of by the following theorem.

THEOREM 5. Let $G = \{a\}$ be a cyclic group of order g, g not prime, and let h be any divisor of g. Then there exists a subgroup H of G whose order is h.

PROOF: Let $g = hj$ and consider the elements $a^j, a^{2j}, \ldots, a^{(h-1)j}, a^{hj} = e$, where e is the identity of G. These elements are all distinct. To verify this statement, suppose the contrary, that is, assume $a^{mj} = a^{kj}$ for distinct integers m and k satisfying $1 \leq m, k \leq h$. Without loss of generality, suppose $m > k$. This implies that $a^{(m-k)j} = e$. Clearly, $m - k < h$ and thus $(m - k)j < hj$. But this is in contradiction to a being the generator of G of order $g = hj$. Since these elements are distinct, they form a subgroup $H = \{a^j\}$ of order h as desired. [5]

Abelian (commutative) groups also satisfy the converse of Lagrange's Theorem. The discussion of this aspect, however, will be postponed until Sylow's Theorem is developed. Sylow's Theorem itself is not needed for this study, but several results, such as the concept of a factor group, which are developed prior to Sylow's Theorem are of use.

CHAPTER 4

SYLOW'S THEOREM

Before stating and proving Sylow's Theorem, it will be necessary to establish several non-trival theorems, the results of which are of significant importance in understanding the proof.

DEFINITION 9. Let G be a finite group and let x and y be any two elements of G. Then x and y are called conjugate elements in G if there is some element g in G such that $g^{-1}xg = y$.

DEFINITION 10. If a is a fixed element in a finite group G, then the set of all those elements of G which are conjugate to a is said to be a class of conjugate elements and is denoted (a).

THEOREM 6. If G is a finite group then G can be resolved into disjoint classes of conjugate elements such that $G = (a_1) + (a_2) + \dots + (a_k)$ where $a_1, a_2, \dots, a_k$ are distinct elements of G.

PROOF: Suppose the classes (a_i) and (a_j) are not disjoint where $1 \leq i, j \leq k$. Hence there are elements g_1 and g_2 in G such that $g_1^{-1}a_ig_1 = g_2^{-1}a_jg_2$. But this implies that $a_i = g_1g_2^{-1}a_jg_2g_1^{-1}$. Thus $a_i \in (a_j)$ and hence $(a_i) \subset (a_j)$. Similary, $a_j \in (a_i)$ and then $(a_j) \subset (a_i)$ implying that $(a_i) = (a_j)$. G is exhausted by these classes since $a \in (a)$ for all a in G.

Consider now a group G and any set of elements in G, say s. Let H be some subgroup of G. Then the set N of all elements h in H such that $h^{-1}Sh = S$ is called the normalizer of S in H. Becoming even more restrictive, the centralizer C of S in H is defined to be the set of all elements h in H such that $h^{-1}sh = s$ for all s in S. It is clear that if S consists of a single element s, then the normalizer and centralizer

are identical sets. In general, the centralizer C will be contained in the normalizer N. In the case where H = G, the centralizer of G in G is called the center of G. Thus the center of G consists of all those elements which commute with every other element of G. It is easily shown that both the normalizer and the centralizer of a set are subgroups of the group. Proof of the former will now be given. The centralizer is shown to be a subgroup in a similar manner.

THEOREM 7. The normalizer N of any set S of elements of a group G is a subgroup of G.

PROOF: By definition, N consists of precisely those elements g of G such that $g^{-1}Sg = S$, that is, $gS = Sg$. Suppose x and y belong to N. Then $(xy)S = x(yS) = x(Sy) = (xS)y = (Sx)y = S(xy)$ and hence xy is also an element of N. If $x \in N$ then $xS = Sx$ implying that $Sx^{-1} = x^{-1}S$ and therefore $x^{-1} \in N$. Thus N is indeed a subgroup of G.

It is now necessary to establish two small lemmas before proving the next theorem.

LEMMA 2. Every finite group G of composite order has proper subgroups.

PROOF: If G is cyclic then proof is complete by Theorem 4. Otherwise suppose G is not cyclic. Then no single element generates the whole group G. Thus if g is any element of G and $g \neq e$ the identity of G, then the cyclic subgroup $\{g\}$ generated by g is a proper subgroup of G.

In the proof of the following Lemma, the statement that a non-empty subset H of a finite group G is a subgroup of G if and only if $H^2 = H$ will be used. This is easily verified and therefore the proof will be omitted here.

LEMMA 3. If H and S are subgroups of a finite group G then C = HS is a group if and only if H and S commute.

PROOF: First note that HS consists of all pairs of elements hs where $h \in H$ and $s \in S$. Suppose C = HS is a group. Let $h \in H$ and $s \in S$. Then $h^{-1} \in H$ and $s^{-1} \in S$, and hence $h^{-1}s^{-1} \in C$ by definition. Since C is a group $(h^{-1}s^{-1})^{-1} = sh \in HS$ implying that $SH \subset HS$. Similary, $HS \subset SH$ and hence HS = SH.

Conversely, suppose HS = SH. Then $C^2 = (HS)(HS) = H(SH)S = H(HS)S = H^2S^2 = HS$. Therefore C = HS is a group. The statement preceeding this Lemma is actually used twice. [5]

With these lemmas, it is now possible to treat a theorem of particular importance.

THEOREM 8. If G is an abelian group of order g and if p is any prime factor of g, then G contains at least one element of order p.

PROOF: The proof is trivial if p = g, so assume that g is composite and continue by induction on g. By Lemma 2, G possesses proper subgroups. Select from these subgroups one proper subgroup H of maximum order $h < g$. (There may be more than one such subgroup but only one is needed.) Two cases must be considered. First suppose p is a divisor of h. By the induction assumption, H then contains an element x of order p, that is, $x^p = e$, where e is the identity of G. But $x \in G$ also, and hence proof is complete.

In the other case, suppose h and p are relatively prime. This means that the only integers which divide both h and p are ± 1. Since H is a proper subgroup of G, there exists an element y of G which is not also an element of H. Let y be of order t, and consider the product

$H\{y\}$. Since G is abelian, $H\{y\} = \{y\}H$ and hence by Lemma 3, $H\{y\}$ is a subgroup of G. Clearly, $H\{y\} \supset H$. But H was assumed to be a subgroup of maximum order. Thus $G = H\{y\}$. The order of $H\{y\}$ is $\frac{ht}{d}$, where d is the order of the intersection of H and $\{y\}$. Therefore, $gd = ht$ and p is a divisor of gd since p is a divisor of g itself. Thus p must also be a divisor of ht. Since p and h are relatively prime, p must be a divisor of t, that is, $t = pq$ for some integer q. The element y^q is then of order p since $(y^q)^p = y^t = e$. [3]

Two additional concepts are now needed. Recall that the center of any group G consists of all those elements z of G such that $zx = xz$ for all other x of G. In particular, the center of G is an abelian subgroup of G.

Now consider the cosets of a normal subgroup of a group. The next theorem gives the following result.

THEOREM 9. The cosets of any normal subgroup N of a group G form a group under multiplication.

PROOF: Form the left decomposition of G by N and hence obtain $G = N + Nx_2 + \ldots + Nx_r$, where $x_1 = e$, $x_2, \ldots, x_r$ are all elements of G. Define the multiplication of cosets as follows: $(Nx)\cdot(Ny) = N(xy)$. This operation gives closure obviously. $(Nx)\cdot(Ne) = N(xe) = Nx$ implying that the coset $N = Ne$ is the left identity of the system of cosets.

$(Nx)\cdot(Ny)\cdot(Nz) = N(xy)\cdot(Nz) = N(xyz) = (Nx)\cdot N(yz) = (Nx)\cdot(Ny)\cdot(Nz)$

and thus the associative law is established. $(Nx^{-1})\cdot(Nx) = N(x^{-1}x)$ $= Ne = N$ establishing the existence of left inverses. [1]

Such a group of cosets is called the factor group of G with respect to N and is denoted by G/N.

The preliminary tools have now been established for satisfactorily

proving Sylow's Theorem. This theorem gives the nearest approximation to the converse of Lagrange's Theorem that is possible, as the counter-examples exhibited clearly show.

SYLOW'S THEOREM. Let G be a group of order g. Let p^m be a divisor of g such that p^{m+1} is not a divisor of g, where p is a prime and m is some positive integer. Then G contains at least one subgroup of order p^m.

PROOF: If g = 1 or g = 2 the proof is trivial. Henceforth, proceed by induction on g. Let $g = p^m q$, where p and q are necessarily relatively prime. By Theorem 5 resolve G into disjoint classes of conjugate elements so that $G = (a_1) + (a_2) + \ldots + (a_k)$. Thus, $g = h_1 + h_2 + \ldots + h_k$, where for $i = 1,2,\ldots,k$, h_i is the number of elements in the corresponding (a_i). Recall also that the normalizer N_i of each a_i is a group. Also it is easy to verify that the order n_i of N_i is $\frac{g}{h_i}$. Now consider two cases. First suppose that $h_\ell > 1$ for some ℓ, $1 \leq \ell \leq k$, and that h_ℓ and p are relatively prime. Since $n_\ell = g/h_\ell$ this implies $n_\ell < g$ clearly. Also, since p^m is a divisor of $g = n_\ell h_\ell$ and p^m does not divide h_ℓ it must divide n_ℓ. By the induction hypothesis the theorem is true for the subgroup N_ℓ, the normalizer of a_ℓ. Hence N_ℓ possesses a subgroup of order p^m which is also a subgroup of G.

In the other case, assume that for all h_i that either $h_i = 1$ or p is a divisor of h_i, where $i = 1,2,\ldots,k$. It is clear from preceding remarks that the classes (a_i) which correspond to $h_i = 1$ are simply classes of self-conjugate elements. At least one such class exists, namely the class (e), where e is the identity of G. Let z then denote the exact number of self-conjugate elements, that is, z is the order of the center of the group. Hence $g = p^m q = z + xp$ for some integer p.

Thus, p necessarily divides z, implying the order of the center of G is divisible by a prime. By Theorem 7, the center Z of G, and thus G too, contains an element of order p, say y, which commutes with all the elements of G. Hence the cyclic group generated by y is a normal subgroup of G. The factor group $G/\{y\}$ is then of order $\frac{p^m q}{p} = p^{m-1}q$. By the induction hypothesis $G/\{y\}$ contains a subgroup of order p^{m-1}. This subgroup may be written in the form $H/\{y\}$, where H is a subgroup of G of order h. Hence $p^{m-1} = \frac{h}{p}$ or $h = p^m$. Therefore, H is the subgroup of G of order p^m corresponding to p, as desired. [5]

CHAPTER 5

THE ABELIAN CASE

Consider now a normal subgroup H of a group G such that the order of H is h. It is easily verified that if the factor group G/H contains a subgroup S of order s, then G contains a corresponding subgroup of order sh. To confirm this, one need only look at the elements of G in the s factors of G/H, where each factor contains h elements. There are then a total of sh elements of G and these elements do in fact form a subgroup of G. Hence the following result:

THEOREM 10. If the order n of an abelian group G is divisible by an integer m, the G contains a subgroup of order m.

PROOF: The theorem is clearly true for small values of n, namely one, two, and three, since these numbers fall into the prime category. The proof will proceed then by induction on n, that is assume that the theorem is true for groups whose orders are less than n. Let p be a prime factor of m, implying also that p is a prime factor of n. But G is abelian by hypothesis. Hence, by Theorem 8, G contains an element of order p, which clearly generates a subgroup, say H, of G of order p. H is normal also since G is abelian. Consider now the abelian factor group G/H, whose order is $\frac{n}{p}$. Note that $\frac{n}{p}$ is strictly less than n, and $\frac{m}{p}$ is a divisor of $\frac{n}{p}$ since m is given to be a divisor of n. By induction assumption then, G/H contains a subgroup of order $\frac{m}{p}$. From the remarks preceeding the theorem, G contains a corresponding subgroup of order $(\frac{m}{p})p = m$, which is the desired subgroup.

CHAPTER 6

SOME CONSEQUENCES OF SYLOW'S THEOREM

The following theorem, due to Cauchy, has already been proved for the abelian case. It is also true in general.

THEOREM 11. Let G be a finite group and let p be a prime factor of the order of G. Then G contains at least one element of order p.

PROOF: Let H be a Sylow subgroup of G of order p^m. If x is any element of H except the identity, then the order of x is of the form p^u, where u is greater than zero. If $u = 1$, then the proof is complete since $x^p = e$ and x is the desired element. Hence $1 < u \leq m$. Let $g = h^{p^{u-1}}$. Then $g^p = h^{p^u} = e$ and g is the element of order p.

Let G be a group of order n, and let p be a prime such that p^m divides n, but p^{m+1} does not divide n, for some integer m. Sylow's Theorem guarantees the existence of at least one subgroup of order p^m. A natural question now arises concerning the possible existence of more than one of these subgroups of order p^m, and if there are more than one, are there any similarities or differences in their composition? In reply, first note that if H is a subgroup of order p^m, then for any element x of G, $x^{-1}Hx$ is also a subgroup of order p^m. More generally, all subgroups which are conjugate with H are, in fact, Sylow subgroups of order p^m.

Recall now that, in the decomposition of G into right or left cosets of a subgroup H, the property that these cosets were either identical or disjoint was of primary importance. It is an interesting generalization that, any time a collection of subsets of a group G

has this property of being disjoint or identical, G may be decomposed into such subsets.

LEMMA 4. Let G be a group and let H and S be subgroups of G. Then for fixed elements x and y of G, any two of the subsets of G of the form HxS and HyS are either identical or disjoint.

PROOF: Suppose HxS and HyS have an element in common. Then for h_1, $h_2 \in H$ and s_1, $s_2 \in S$, $h_1xs_1 = h_2ys_2$. Hence $H(h_1xs_1)S = H(h_2ys_2)S$. But H and S are subgroups implying $Hh_1 = Hh_2 = H$ and $s_1S = s_2S = S$. Thus HxS = HyS.

It is not difficult now to establish a pattern by which G can be decomposed into disjoint subsets of the type just discussed. Simply pick an element g_1 in G and construct Hg_1S. If this subset is not the whole of G, pick an element g_2 of G which is not in Hg_1S and construct Hg_2S. Continue in this manner until every element of G is in one of these subsets. Then $G = Hg_1S + Hg_2S + \dots + Hg_rS$ is the desired decomposition of G.

The original questions will now be answered by the following theorem:

THEOREM 12. All Sylow subgroups associated with the same prime p are conjugate to one another, that is all Sylow subgroups of the same prime p form a complete conjugate class.

PROOF: Let H and S be subgroups of order p^m. Form the decomposition of G relative to H and S as constructed above. Then $G = Hx_1S + Hx_2S + \dots + Hx_rS$. If the order of G is g, then $g = \frac{p^m p^m}{d_1} + \frac{p^m p^m}{d_2} + \dots + \frac{p^m p^m}{d_r}$,

where for $1 \leq i \leq r$, d_i is the order of the subgroup $x_i^{-1}Hx_i \cap S \equiv D_i$.

(D_i is a subgroup for each i since it is the intersection of two subgroups.)

But $g = p^m g'$, where g' and p relatively prime. Hence,

$$g'p^m = \frac{p^m p^m}{d_1} + \frac{p^m p^m}{d_2} + \ldots + \frac{p^m p^m}{d_r} \quad \text{implying that } g' = \frac{p^m}{d_1} + \frac{p^m}{d_2} + \ldots + \frac{p^m}{d_r}.$$

Now it is easily shown that for each i, D_i is a subgroup of S. Hence the order d_i of D_i, must be of the form p^u where $0 \leq u \leq m$. Hence either $\frac{p^m}{d_i} = p^{m-u} \neq 1$ or $\frac{p^m}{d_i} = 1$. But since g' and p are relatively prime, there must be at least one term on the right hand side of the equation such that $\frac{p^m}{d_j} = 1$, that is, $p^m = d_j$, for some j.

But since $D_j \subset S$ and the order of S is also p^m, it follows that $D_j = S$. By a similar argument, it may be shown that $D_j = x_j^{-1} H x_j$ and therefore $x_j^{-1} H x_j = S$, or H and S are conjugate. [5]

A direct consequence of this theorem is that a Sylow subgroup is unique if and only if it is a normal subgroup of G. Another important aspect of Sylow's subgroups belonging to one prime concerns the number of them that may possibly exist. A treatment of this topic is given by the next theorem.

THEOREM 13. The number K of Sylow subgroups of a group G corresponding to a prime p is of the form $1 + p\ell$, for some integer ℓ. Also, K is a factor of the order of G.

PROOF: Let H be a fixed Sylow subgroup corresponding to the prime p. Then the order of H is p^m, for some integer m. Let N be the normalizer of H in G. Recall that N consists of all those elements x of G such that $x^{-1} H x = H$. From the preceeding theorem, the number K of distinct Sylow subgroups is the same as the number of distinct subgroups of G which are conjugate to H. If n is the order of N and g is the order of G, then it has been shown in previous material that $g = nK$, where K

also corresponds to the index of N in G. Hence K is a factor of g.

For every element h of H, $h^{-1}Hh = H$, since H is a subgroup of G. Thus h is also an element of N, implying that H is contained in N. In fact, H is a normal subgroup of N. Now n is a divisor of g and n is not divisible by p^{m+1} since g is not divisible by p^{m+1}. But the order p^m of H must be a factor of n. Hence $n = p^m n'$, where n' and p are relatively prime. Construct the decomposition of G relative to H and N such that $G = Hx_1N + Hx_2N + \dots + Hx_rN$. Then

$g = \frac{p^m n}{d_1} + \frac{p^m n}{d_2} + \dots + \frac{p^m n}{d_r}$ where, for $1 \leq i \leq r$, d_i is the order of $x_i^{-1}Hx_i \cap N \equiv D_i$. Without loss of generality, assume $x_1 = e$, the identity of G. Then $Hx_1N = HeN = HN = N$, since H N. Hence $\frac{p^m n}{d_1} = n$ implying that $d_1 = p^m$. Note that no other term in the decomposition of G can have the property of being identical to N. This is true by the nature of the decomposition itself. Hence $g = nK = n + \frac{p^m n}{d_2} + \dots + \frac{p^m n}{d_r}$, or $K = 1 + \frac{p^m n}{d_2} + \dots + \frac{p^m n}{d_r}$. As noted previously, for $1 \leq i \leq r$, D_i is a subgroup of the group $x_i^{-1}Hx_i$. But the order of $x_i^{-1}Hx_i$ is the same as the order of H, that is, the order of $x_i^{-1}Hx_i$ is p^m. The order of D_i must divide the order of $x_i^{-1}Hx_i$ which implies that $\frac{p^m}{d_i}$ is of the form p^u, for $0 \leq u \leq m$. The proof will be completed when it is shown that $u > 0$ for all terms of the form $\frac{p^m}{d_i}$, except the first.

To this end suppose that for some j, $2 \leq j \leq r$, $d_j = p^m$. This implies that $D_j = x_j^{-1}Hx_j$ by the same argument used in the proof of Theorem 12. But D_j is a subgroup of N; hence the result that $x_j^{-1}Hx_j$ is contained in N. It has been noted that p^m is the highest power of p which divides n, the order of N. Hence by Sylow's Theorem, N possesses one or more Sylow subgroups of order p^m. The existence of

at least two has been established already, namely H and $x_j^{-1}Hx_j$. But H is normal in N and hence is unique. Therefore, $H = x_j^{-1}Hx_j$ implying that x_j is an element of N. But this leads to the result that $Hx_jN = HN = N$. As was noted, this is impossible unless $x_j = e = x_1$. Hence all the terms on the right-hand side of $K = 1 + \frac{p^m}{d_2} + \ldots + \frac{p^m}{d_r}$ are divisible by p, except the first, that is $K = 1 + p\ell$ for some integer ℓ . [5]

CHAPTER 7

RELATED EXAMPLES

Much information can be obtained about a group from a study of its p-Sylow subgroups. Unfortunately, these p-groups can be quite complicated, as the following sequence of examples will illustrate.

Consider first a collection of groups, all of whose orders are a power of two. There is only one possible group of order two. It is necessarily cyclic and hence Abelian also. Both groups of order four are Abelian. One of these is a cyclic group generated by an element of order four. The other group consists of the elements e, a, b, and ab (e being the identity). In this group $a^2 = b^2 = e$ and ab = ba. This latter group is frequently called the Four-Group or the Quadratic Group. Of the five possible groups of order eight, three are Abelian and two are non-Abelian. One possibility is the cyclic group generated by an element of order eight. Another Abelian group is generated by two elements, say a and b, where $a^4 = b^2 = e$ and ab = ba. The third Abelian group is generated by three elements, call them a, b, and c. In this particular group the following relations hold: ab = ba, bc = cb, ca = ac, and $a^2 = b^2 = c^2 = e$. The two non-Abelian groups of order eight are the so-called Dihedral Group and the Quaternion Group. Two elements, say a and b, and satisfying $a^4 = b^2 = e$ and $ba = a^3b$, generate the Dihedral Group, while if a and b are the generating elements of the Quaterion Group, then $a^4 = e$, $a^2 = b^2$, and $ba = a^3b$.

It should be noted here that the method of proving that these groups are the only ones of order eight is merely a process of elimination in which all the possible combinations of elements are

considered under the restrictions of the group definition. As might be assumed, such a method becomes quite tedious as the order of the group increases. Also, as illustrated above, the variety of the groups obtained increases greatly as both the prime being considered and its power increase. Indeed, the investigation of p-Sylow subgroups is not at all trivial.

Consider now a finite group G and a prime p which divides the order of G. Suppose x and y are elements of G of order p. It might be both useful and desirable to conclude in general that the product xy has order p or even some power of p. This result however can not be obtained. Let G be a group of order six generated by the elements a and b, where $a^3 = b^2 = e$ and $ba = a^2b$. Then both b and ab are of order two, but b(ab) is of order three, clearly not a power of two.

In an abelian group, the p-Sylow subgroup associated with a prime p is unique. The converse of this statement however is not true. A counter-example is easily obtained. In the group of order six described above, there are three p-Sylow subgroups associated with the prime two. They are $\{e,b\}$, $\{e,ab\}$, and $\{e,a^2b\}$.

And so, the reduction of finite groups to p-Sylow subgroups is beneficial. However, the p-Sylow subgroups themselves may be quite complicated and may not, at times, lend themselves easily to desirable generalizations.

This concludes the discussion of Sylow's Theorem, its development and more immediate consequences.

BIBLIOGRAPHY

1 Birkhoff, G. and MacLane, S., A Survey of Modern Algebra, Revised Edition, New York: Macmillan Company, 1953.

2 Carmichael, R.D., Groups of Finite Order, Dover Edition, Dover: Dover Publications, Inc., 1956.

3 Hall, M. Jr., The Theory of Groups, First Edition, New York: Macmillan Company, 1959.

4 Kurosh, A.G., Lectures on General Algebra, translated by K.A. Hirsch, New York: Chelsea Publishing Company, 1963.

5 Ledermann, W., Introduction to the Theory of Finite Groups, Third Revised Edition, New York: Interscience Publishers, Inc., 1957.

6 McCoy, N.H., Introduction to Modern Algebra, Third Printing, Boston: Allyn and Bacon, Inc., 1960.

VITA

Jack O. Beamer, son of Mr. and Mrs. Blaine O. Beamer, was born on June 11, 1939, in Harrisburg, Pennsylvania. He attended Susquehanna Township Junior Senior High School in Progress, Pennsylvania, from which he graduated in 1958. In 1962 he received his Bachelor of Science degree in Mathematics, with departmental honors, from Juniata College, Huntingdon, Pennsylvania. In September of 1962 he entered the Graduate School of Lehigh University as a graduate assistant in the Department of Mathematics and Astronomy, and has maintained this position to the present time.